Sums and Products of Distinct Sets and Distinct Elements in Fields of Characteristic 0

Karsten O. Chipeniuk [1]

Department of Mathematics, University of British Columbia, 1984 Mathematics Road, Vancouver, B.C. V6T 1Z2 Canada

Abstract

Let A and B be finite subsets of an algebraically closed field K of characteristic 0 such that $|B| = C|A|$. We show the following variant of the sum product phenomena: If $|AB| < \alpha|A|$ and $\alpha, C, \alpha/C \ll \log|A|$, then $|kA + lB| \gg |A|^k|B|^l$. This is an application of a result of Evertse, Schlickewei, and Schmidt on linear equations with variables taking values in multiplicative groups of finite rank, in combination with an earlier theorem of Ruzsa about sumsets in $\mathbb{R}^d$. As an application of the case $A = B$ we give a lower bound on $|A^+| + |A^\times|$, where A^+ is the set of sums of distinct elements of A and $A^\times$ is the set of products of distinct elements of A.

1 Introduction

Let A be a finite subset of a commutative ring R. Then we can form the sumset $2A = A + A = \{a + a' : a, a' \in A\}$ and the productset $A^2 = A \cdot A = \{aa' : a, a' \in A\}$, as well as the iterated variant kA of the sumset, for $k \in \mathbb{Z}^+$. In addition, letting $A = \{a_1, \ldots, a_n\}$, we can take the set of all sums of, and the set of all products of, distinct elements of A, respectively

$$A^+ = \left\{ \sum_{i=1}^{n} \epsilon_i a_i : \epsilon_i \in \{0, 1\},\ \forall\, i = 1, \ldots, n \right\} \tag{1}$$

and

$$A^\times = \left\{ \prod_{i=1}^{n} a_i^{\epsilon_i} : \epsilon_i \in \{0, 1\},\ \forall\, i = 1, \ldots, n \right\} \tag{2}$$

We are then led to consider

$$g_R(N) = \min_{A \subset R,\ |A|=N} \{|A^+| + |A^\times|\}. \tag{3}$$

Such expressions were investigated by Erdös and Szemerédi in [5] in the integer setting. They showed that

$$g_{\mathbb{Z}}(N) < N^{c\frac{\log N}{\log\log N}} \tag{4}$$

[1] Correspondence may be directed to:
Email: karstenc@math.ubc.ca
Phone: 1 604 822 3887
Fax: 1 604 822 6074
The author was supported by an NSERC Postgraduate Scholarship.

for some absolute constant $c > 0$. Later Chang proved ([2]) their conjecture that this essentially provides the lower bound as well; more precisely, she showed that

$$g_{\mathbb{Z}}(N) > N^{(1/8-\epsilon)\frac{\log N}{\log\log N}}. \tag{5}$$

More recently, in [3], Chang addressed a question of Ruzsa, proving that $g_{\mathbb{C}}(N)$ grows faster than any power of N,

$$\lim_{N\to\infty} \frac{\log(g_{\mathbb{C}}(N))}{\log N} = \infty. \tag{6}$$

In this article we will obtain an explicit lower bound for $g_K(N)$ in an algebraically closed field K of characteristic 0. In particular, since $g_{R_2}(N) \leq g_{R_1}(N)$ whenever R_1 is a subring of R_2, this bound will hold for any field of characteristic 0. Our result in this direction is the following.

Theorem 1 (Lower bound on $g_K(N)$)**.** *For any $\epsilon > 0$ and any N sufficiently large we have*

$$g_K(N) \geq N^{(1/264-\epsilon)\frac{\log\log(N)}{\log\log\log(N)}}.$$

The proof largely follows that of [2]. This approach uses a manifestation of the sum-product phenomena, namely that a small productset requires a large iterated sumset. We will use a version which holds in the field K.

Theorem 2. *Let $A \subset K$ be finite, and suppose that $|A^2| \leq \alpha|A|$. Then for any integer $h \geq 2$ we have*

$$|hA| \geq e^{(-h^{65h}(\alpha+1))}|A|^h.$$

This result was in essence also proved by Chang in [4], without the explicit dependence on h, which will be essential in the proof of 1. Using a result of Ruzsa ([7], Theorem 14 below), we have also extended this result to distinct sets A and B. Namely, for $A, B \subset K$, define AB, $A+B$, and $kA+lB$ in the obvious manner. Then we have

Theorem 3 (Small productset implies large iterated sumset for distinct sets)**.** *Let $A, B \subset K$ with $|B| = C|A|$, and suppose that $|AB| < \alpha|A|$. If*

$$\max\left(\alpha, C, \frac{\alpha}{C}\right) \leq \frac{1}{(k+l)^{65(k+l)}} \log|A|$$

then

$$|kA + lB| \gg_{k,l} |A|^k|B|^l. \tag{7}$$

The proofs of Theorems 2 and 3 rely on bounding the number of additive tuples in A^k (respectively, $A^k \times B^l$); this is approached via an induction using a result of Evertse, Schlickewei, and Schmidt [6] which we next describe.

Let $K^* = K \setminus \{0\}$ be the multiplicative subgroup of nonzero elements in K. Let Γ be a subgroup of $(K^*)^d$ with rank r (so the minimum number of elements from which we can

generate Γ is r). For coefficients $a_1, \ldots, a_d \in K$ let $A(d, r)$ denote the number of solutions $(x_1, \ldots, x_d) \in \Gamma$ to

$$a_1x_1 + a_2x_2 + \cdots + a_dx_d = 1$$

which are nondegenerate (namely, no proper subsum of the left side vanishes). Note that in the following, the bound is finite and depends only on r and d, and not on the particular group Γ nor the particular coefficients of the objective equation.

Theorem 4 (Linear equations have few solutions in a multiplicative group)**.** [6]

$$A(d, r) \leq \exp\left((6d)^{3d}(r + 1)\right).$$

We will also use two other standard tools of additive combinatorics (see, for example, [9]). The first is Freiman's theorem in torsion-free groups.

Theorem 5 (Freiman's Theorem)**.** *Let Z be a torsion-free abelian group, and let $A \subset Z$ with $|A + A| \leq K|A|$ for some $K \in \mathbb{R}$. Then there exists a proper generalized arithmetic progression P of dimension at most $K - 1$ and size $|P| \leq C(K)|A|$ which contains A. Here $C(K)$ depends only on K.*

The second is the Plünnecke-Ruzsa Inequality, in a version due to Ruzsa [8].

Theorem 6 (Plünnecke-Ruzsa Inequality)**.** [8] *Let Z be an abelian group and let $A, B \subset Z$ with $|A + B| \leq K|A|$. Then for every $n, m \in \mathbb{N}$ we have $|nB - mB| \leq K^{n+m}|A|$.*

Acknowledgements: The author would like to thank József Solymosi for pointing out and providing the reference [6], and Izabella Łaba for her constant support throughout the production of this work.

2 Proof of Theorem 2

Let $A \subset K$ be finite with $|A| = n$ and $|A^2| \leq \alpha|A|$.

We begin by extending a definition from [2]. In particular, consider $A^* := A \setminus \{0\} \subset K^*$. Then we define the multiplicative dimension of A, denoted $\dim_\times(A)$ to be the minimal number m such that A^* is contained in a subgroup of K^* of rank m. In other words,

$$\dim_\times(A) = \min\{M : \exists\, z_1, \ldots, z_M \in K^* \text{ such that } A^* \subset \langle z_1, \ldots, z_M \rangle\}. \tag{8}$$

We have the following two properties.

Lemma 7 (Multiplicative Dimension)**.** *Let $A \subset K$ be finite, and suppose A has multiplicative dimension m.*

(a) $m \leq |(A^*)^2|/|A^*|$

(b) *If $A^* \subset \langle z_1, \ldots, z_m \rangle := G$, there is an isomorphism $\nu : G \to (\mathbb{Z}^m, +)$. Moreover, $\nu(A^*)$ is m-dimensional (that is, when viewed as a subset of $\mathbb{R}^m$ the smallest dimension subspace it may be contained in has full dimension)*

Proof. (a) Let $\beta = |(A^*)^2|/|A^*|$. Since K^* is abelian, Chang's refinement of Freiman's theorem applies ([1], stated for torsion free groups in [9]), and we may contain A^* in a progression in K^* of dimension $\lfloor \beta - 1 \rfloor$, say

$$A \subset \left\{ z_1 \prod_{i=2}^{\lfloor \alpha - 1 \rfloor + 1} z_i^{j_i} : 0 \leq j_i \leq k_i - 1 \right\}.$$

But the right hand side is clearly a subset of $\langle z_1, \ldots, z_{\lfloor \alpha - 1 \rfloor + 1} \rangle$, which clearly has fewer than α generators.
(b) By the fundamental theorem of finitely generated abelian groups applied to $\langle z_1, \ldots, z_m \rangle$, there is such an isomorphism. Minimality of m implies the full dimensionality of A. □

Note that if $0 \in A$, then

$$\begin{aligned} |(A^*)^2| &= |A^2 \setminus \{0\}| \\ &= |A^2| - 1 \\ &\leq \alpha|A| - 1 \\ &= \alpha(|A^*| + 1) - 1 \\ &< \alpha|A^*|. \end{aligned}$$

Hence Theorem 2 is an easy corollary of the following.

Proposition 8 (Iterated Sum-Product)**.** *Let $A \subset K$ be finite, and suppose that* $\dim_\times(A) = m$. *Then for any $h \geq 2$ we have*

$$|hA| \geq e^{(-h^{65h}(m+1))}|A|^h$$

To prove Proposition 8 we seek to bound the number of solutions to the equation

$$x_1 + \cdots + x_h = x_{h+1} + \cdots + x_{2h}$$

where $x_i \in A$ for each i. In the case $A = -A$, we may rewrite this equation as $x_1 + \cdots + x_{2h-1} + x_{2h} = 0$. If we further assume $0 \notin A$, then we are free to apply Theorem 4 to A. The result is the following statement, similar to a lemma of Chang in [4]:

Lemma 9. *Suppose that A satisfies $A = -A$ and $0 \notin A$. For every $k \geq 2$ there is n sufficiently large that*

(a) *The number of solutions $(y_1, \ldots, y_k) \in A^k$ to $y_1 + \cdots + y_k = 1$ is at most $e^{k^{12k}(m+1)} n^{\lfloor k/2 \rfloor}$ if k is odd and $e^{k^{12k}(m+1)} n^{k/2-1}$ if k is even.*

(b) *The number of solutions $(y_1, \ldots, y_k) \in A^k$ to $y_1 + \cdots + y_k = 0$ is at most $e^{k^{12k}(m+1)} n^{\lfloor k/2 \rfloor}$.*

Proof. The proof follows the same line that of the lemma in [4]. The main difference now is that we keep track of all constants. Let $D_{t,m} := \exp(t^{12t}(m+1))$. In addition, let

$$\gamma_1(t) = \begin{cases} \lfloor t/2 \rfloor, & \text{if } t \text{ is odd} \\ t/2 - 1, & \text{if is even} \end{cases} \tag{9}$$

$$\gamma_0(t) = \lfloor t/2 \rfloor. \tag{10}$$

Hence we are trying to show that the number of solutions to $y_1 + \cdots + y_k = 1$ is at most $D_{k,m} n^{\gamma_1(k)}$ and the number of solutions to $y_1 + \cdots + y_k = 0$ is at most $D_{k,m} n^{\gamma_0(k)}$.

Base Case: When $k = 2$ we see directly that the number of solutions to $y_1 + y_2 = 0$ is at most n (Each of $|A|$ choices for y_1 gives one possibility for y_2), while the number of nondegenerate solutions to $y_1 + y_2 = 1$ is at most $\exp((12)^6(2m+1))$ by Theorem 4, and the only two possible degenerate solutions are $(0, 1)$ and $(1, 0)$. We have

$$\exp((12)^6(2m+1)) + 2 \leq \exp(2^{24}(m+1)).$$

Hence the bound holds for $k = 2$.

Induction: Let $k > 2$ be fixed, and suppose both parts of the theorem have been proved for each integer less than k.

We begin with the equation $y_1 + \cdots + y_k = 0$, which we rewrite as $z_1 + \cdots + z_{k-1} = 1$ by fixing a value of $-y_k$, dividing through by it, and rearranging. There are still n possibilities for each variable in this equation, and each still falls in G since G is closed under division.

First suppose k is even. Then $k - 1$ is odd, so by the inductive hypothesis there are at most $D_{k-1,m} n^{(k-2)/2}$ solutions to the latter equation, and therefore $D_{k-1,m} n^{k/2}$ solutions to the original. Since k is even, this is the desired result.

Next, if k is odd, $k - 1$ is even, and the latter equation has fewer than $D_{k-1,m} n^{(k-1)/2-1}$ solutions, whereby the original has fewer than $D_{k-1,m} n^{(k-1)/2}$. This again gives the desired result.

Hence the result for zero sums holds for k.

To count solutions to $y_1 + \cdots + y_k = 1$, we begin by applying the Theorem 4. This tells us that the number of nondegenerate solutions in the entirety of the rank km group G^k is bounded by $\exp((6k)^{3k}(km+1))$. We use the inductive hypothesis to count degenerate solutions. But this reduces to computing, for each t, $2 \leq t \leq k - 1$, the number of solutions to the pair of equations

$$\sum_{j=1}^{t} y_{i_j} = 0$$

$$\sum_{j=t+1}^{k} y_{i_j} = 1$$

where $i_1, \ldots, i_k$ is some permutation of $1, \ldots, k$ with $i_1 < \cdots < i_t$ and $i_{t+1} < \cdots < i_k$.

Since there are $\binom{k}{t}$ choices for $\{i_1, \ldots, i_t\}$, the total number of solutions is bounded via the induction by

$$2\sum_{t=2}^{k-1}\binom{k}{t}D_{t,m}D_{k-t,m}n^{\gamma_0(t)+\gamma_1(k-t)}$$

where we have used the extra factor of two to simply account for the small number nondegenerate solutions. We begin by computing the exponent. We can easily compute that for k even we have

$$\gamma_0(t) + \gamma_1(k-t) = k/2 - 1. \tag{11}$$

Similarly, for k odd, we get

$$\gamma_0(t) + \gamma_1(k-t) = \begin{cases} (k-1)/2, & \text{if } t \text{ is even} \\ (k-3)/2, & \text{if } t \text{ is odd} \end{cases}. \tag{12}$$

In both cases we see that we can bound the number of solutions by

$$\left(2\sum_{t=2}^{k-1}\binom{k}{t}D_{t,m}D_{k-t,m}\right)n^{\gamma_1(k)} \tag{13}$$

and we need only compute the constant.

Now,

$$D_{t,m}D_{k-t,m} = \exp\left[(t^{12t} + (k-t)^{12(k-t)})(m+1)\right]. \tag{14}$$

The exponent is maximized over all possible values of t for $t = k-1$.

The entire sum is therefore bounded above by

$$2\exp((1 + (k-1)^{12(k-1)})(m+1))\sum_{t=2}^{k-1}\binom{k}{t} \leq \exp(k^{12k}(m+1))$$

using the fact that $\sum_{t=2}^{k-1}\binom{k}{t} < 2^k$.

Hence the result follows by induction. □

Now, if $A \neq -A$, we simply extend A to $A' = A \cup (-A)$. This increases the size of our objective set to at most $2n$, while increasing the rank of the ambient subgroup G by at most 1 (adding -1 as a generator). Hence the rank of G^k increases by at most k.

There are fewer solutions to $x_1 + \cdots + x_h = x_{h+1} + \cdots + x_{2h}$ in A than there are in A', the latter quantity being bounded by $\exp((2h)^{32h}(m+2))(2n)^h$.

If, in addition, $0 \in A$, the number of solutions we gain is certainly less than

$$\sum_{t=1}^{2h-1}\binom{2h}{t}D_{2h-t,m+1}(2n)^{\lfloor(2h-t)/2\rfloor}$$

Here we have set one or more variables (of which there are $2h$) equal to 0 and used Lemma 9 to count the number of solutions to the resulting equation. We can bound this by

$$\begin{aligned} D_{2h-1,m+1}(2n)^{h-1} \cdot 2^{2h} &\leq 2^{3h-1} \exp((2h-1)^{16(2h-1)}(m+2))n^{h-1} \\ &\leq \exp((2h-1)^{16(2h-1)}(m+1) + 5h)n^{h-1}. \end{aligned}$$

The total possible number of solutions after symmetrizing and adding 0, then, is

$$\begin{aligned} &\leq 2^h \exp((2h)^{32h}(m+2))n^h + \exp((2h-1)^{16(2h-1)}(m+1) + 5h)n^{h-1} \\ &\leq \exp(h^{65h}(m+1))n^h. \end{aligned}$$

We have therefore proved:

Lemma 10 (Additive $2h$-tuples)**.** *The number of additive $2h$-tuples in A, that is the number of solutions in A^{2h} to the equation $x_1 + \cdots + x_h = x_{h+1} + \cdots + x_{2h}$, is bounded above by* $\exp(h^{65h}(m+1))n^h$.

In light of the following lemma from [2] we have proved Proposition 8.

Lemma 11 (Cauchy-Schwarz for iterated sumsets)**.** *Let M denote the number of additive $2h$-tuples in a finite set B, that is the number of solutions in B to the equation $x_1 + \cdots + x_h = x_{h+1} + \cdots + x_{2h}$. Then*

$$|hB| \geq \frac{|B|^{2h}}{M}$$

3 Proof of Theorem 1

We are now in a position to follow the proof in [2], using our revised definition of multiplicative dimension (8) and the bound in Proposition 8. We begin by showing that a large proportion of the iterated sumset hA is covered by sums of h distinct elements.

Lemma 12 (Stirling's formula applied to Lemma 11)**.** *Let $A \subset K$ be finite with multiplicative dimension m and with $|A|$ sufficiently large. Then for any sufficiently large $h \in \mathbb{N}$ with $h \leq |A|$ we have*

$$|hA \cap A^+| \geq \frac{|A|^h}{\exp(h^{66h}(m+1))}.$$

Proof. This follows exactly as in [2]. First we note that the left hand side is the number of simple sums with exactly h summands. Letting

$$r_{hA}(x) = |\{(a_1, \ldots, a_h) \in A^h : a_1 + \cdots + a_h = x\}|$$

we clearly have

$$\binom{|A|}{h} \leq \sum_{x \in hA \cap A^+} r_{hA}(x).$$

Using Stirling's formula in the form $N! \sim N^{N+1/2}e^{-N}$ to write

$$\binom{|A|}{h} = \frac{|A|!}{h!(|A|-h)!} \geq C\frac{|A|^{|A|}}{h^{h+1/2}|A|^{|A|-h}} = C(|A|/h^{1+1/2h})^h.$$

for an absolute constant C. Combining the previous two relations and applying Cauch-Schwartz followed by Proposition 8 we have

$$\begin{aligned} C(|A|/h^{1+1/2h})^h &\leq |hA \cap A^+|^{1/2}\left(\sum_{x\in hA\cap A^+}(r_{hA}(x))^2\right)^{1/2} \\ &\leq |hA \cap A^+|^{1/2}(\exp(h^{65h}(m+1))|A|^h)^{1/2}. \end{aligned}$$

It follows that

$$|hA \cap A^+| \geq C\frac{|A|^h}{h^{2h+1}\exp(h^{65h}(m+1))},$$

and absorbing the constant C and the factor h^{2h+1} into the exponential (for h large) we have

$$|hA \cap A^+| \geq \frac{|A|^h}{\exp(h^{66h}(m+1))}.$$

□

The following replaces Proposition 14 in [2] for our case.

Lemma 13 (Small mult. dim. implies large simple sum)**.** *Let $B \subset K$, $|B| \geq \sqrt{n}$, and denote the multiplicative dimension of B by m. Then for any ϵ_1, $0 < \epsilon_1 < 1/132$, if*

$$m + 1 \leq \left(\frac{1}{132} - \epsilon_1\right)\frac{\log\log(n)}{\log\log\log(n)}$$

then

$$g(B) \geq n^{\epsilon_1 \frac{\log\log(n)}{\log\log\log(n)}}.$$

Proof. We clearly have

$$g(B) > |B^+| \geq |hB \cap B^+|$$

for any $h \in \mathbb{N}$. Applying Lemma 12 we have

$$g(B) > \frac{|B|^h}{\exp(h^{66h}(m+1))}.$$

Now, we take $h = \lfloor \frac{1}{66}\frac{\log\log(n^{1/2})}{\log\log\log(n)} \rfloor$. Then

$$66h\log(h) \leq \log\log(n^{1/2})$$

so

$$\exp(h^{66h}(m+1)) \leq n^{(m+1)/2}.$$

But then we have

$$g(B) > \frac{|B|^h}{n^{(m+1)/2}} \geq n^{h/2-(m+1)/2}$$

Recalling our condition on m and our choice of h we have the result. □

This last lemma reduces us to considering the case where all large subsets of A have large multiplicative dimension,

$$m \geq \lfloor \left(\frac{1}{132} - \epsilon_1 \right) \frac{\log\log(n)}{\log\log\log(n)} \rfloor.$$

Now, recalling Lemma 7, giving $\nu(A)^+$ the obvious meaning we note that

$$|A^\times| = |\nu(A)^+|. \tag{15}$$

To complete the proof of the theorem we follow very closely the argument given in [2].

We divide A into sets $B_1, \ldots, B_{\lfloor \sqrt{n} \rfloor}$, each with size $|B_i| \geq \sqrt{n}$, and then denote $A_s = \cup_{i=1}^s B_i$. We let ϵ_2 satisfy $0 < \epsilon_2 < 1/2$, and we let

$$\rho = 1 + n^{-1/2+\epsilon_2}.$$

The proof now splits into a trivial case, followed by a complementary case in which we are able to effectively use the large multiplicative dimension of the B_is.

First, if $|\nu(A_s \cup B_{s+1})^+| > \rho|\nu(A_s)^+|$ for every s, we can begin with $A_1 = B_1$ and iterate, gaining a factor of ρ each time, to get

$$|\nu(A)^+| > \rho^{\lfloor \sqrt{n} \rfloor - 1}|\nu(B_1)| > \rho^{\sqrt{n}-2}\sqrt{n}.$$

Hence, using (for x small) $\log(1+x) > x - x^2/2 > x/2$ we have

$$\begin{aligned} g(A) &> |A^\times| = |\nu(A)^+| \\ &> \exp((\sqrt{n}-2)\log(\rho) + \frac{1}{2}\log(n)) \\ &> \exp((\sqrt{n}-2)(1/2)n^{-1/2+\epsilon_2} + \frac{1}{2}\log(n)) \\ &> \exp((1/2)n^{\epsilon_2}) \end{aligned}$$

The last bound is clearly much better than what we are trying to prove.

We are therefore reduced to the case where $|\nu(A_s \cup B_{s+1})^+| \leq \rho|A_s^+|$ for some s. Let $m = \dim_\times(B_{s+1})$, so $m \geq \lfloor \left(\frac{1}{132} - \epsilon_1 \right) \frac{\log\log(n)}{\log\log\log(n)} \rfloor$.

Now, since the sets B_i are disjoint, the sets $\nu(B_i)$ are as well, so that

$$\nu(A_s \cup B_{s+1})^+ = (\nu(A_s) \cup \nu(B_{s+1}))^+ = \nu(A_s)^+ + \nu(B_{s+1})^+. \tag{16}$$

We therefore have

$$|\nu(A_s)^+ + \nu(B_{s+1})^+| \leq \rho|\nu(A_s)^+|, \tag{17}$$

so by Plünnecke's Inequality (Theorem 6) for any $h \in \mathbb{N}$ we have

$$|(h+1)\nu(B_{s+1})^+ - \nu(B_{s+1})^+| \leq \rho^{h+2}|\nu(A_s)^+|.$$

But the left hand side is of course larger than

$$\begin{aligned} |h \cdot \nu(B_{s+1})^+| &\geq |\nu(B_{s+1})^+[h]| \\ &\geq h^m. \end{aligned}$$

where setting $\nu(B_{s+1}) = \{b_1, \ldots, b_k\}$ we have defined

$$\nu(B_{s+1})^+[h] := \left\{ \sum_{i=1}^{k} \epsilon_i b_i : \epsilon_i \in \{0, 1, \ldots, h\},\ i = 1, \ldots, k \right\}$$

and in which the second inequality comes from the simple sum of a basis of $\mathbb{Z}^m$ chosen from $\nu(B_{s+1})$ (via Lemma 7). We take $h = \lfloor n^{1/2-\epsilon_2} \rfloor$, so that

$$\begin{aligned} \rho^{h+2} &\leq (1 + n^{-1/2+\epsilon_2})^{n^{1/2-\epsilon_2}+2} \\ &< \exp(n^{-1/2+\epsilon_2}(n^{1/2-\epsilon_2} + 2)) \\ &< e^3. \end{aligned}$$

Combining, we have

$$\begin{aligned} g(A) &> g(A_s) \\ &> |\nu(A_s)^+| \\ &> e^{-3}h^m \\ &> e^{-3}\lfloor n^{1/2-\epsilon_2} \rfloor^{\lfloor \left(\frac{1}{132}-\epsilon_1\right) \frac{\log\log(n)}{\log\log\log(n)} \rfloor}. \end{aligned}$$

This proves the proposition.

4 Sums of Distinct Sets With Small Productset

We now prove Theorem 3. Let $A, B \subset K$ be finite, with $|B| = C|A|$, and suppose that $|AB| < \alpha|A|$. Fix intergers k and l, and assume that

$$\max\left(\alpha, C, \frac{\alpha}{C}\right) \leq \frac{1}{(k+l)^{65(k+l)}} \log|A|.$$

For $S \subset K$ finite, we will denote by G_S some fixed multiplicative group in K^* of rank $\dim_\times S$ which contains S^* (see Lemma 7).

The strategy is to use the condition $|AB| < \alpha|A|$ to bound the multiplicative dimensions of $|A|$ and $|B|$ in terms of α and C. Our main tool will be the following result of Ruzsa [7].

Theorem 14 (Sumsets in $\mathbb{R}^n$)**.** [7] *Let $n \in \mathbb{Z}^+$, and let $X, Y \subset \mathbb{R}^n$, $|X| \leq |Y|$, and suppose* $\dim(X+Y) = n$. *Then we have*

$$|X+Y| \geq |Y| + n|X| - \frac{n(n+1)}{2}. \tag{18}$$

Now, suppose $0 \notin A \cup B$, and let $D = \dim_\times(A \cup B)$. Then by Lemma 7 there is an isomorphism $\nu : G_{A \cup B} \to (\mathbb{Z}^D, +)$. Then we can compute $\nu(A) + \nu(B)$, and set $d = \dim(\nu(A) + \nu(B)) \geq \dim_\times(AB)$. Now, we may have $d < D$, so we cannot immediately apply Theorem 14. However, $\nu(A) + \nu(B)$ contains translates $\nu(A) + \beta$ and $\alpha + \nu(B)$ for $\alpha \in \nu(A)$, $\beta \in \nu(B)$. Letting $\mathbb{A}^d$ be the real affine space containing $\nu(A) + \nu(B)$, we can provide an isomorphism $\eta : \mathbb{A}^d \to \mathbb{R}^d$. Setting $X = \eta(\nu(A) + \beta)$ and $Y = \eta(\alpha + \nu(B))$ we find that

$$\begin{aligned} |X+Y| &= |\eta(\nu(A) + \nu(B) + \alpha + \beta)| \\ &= |\nu(A) + \nu(B) + \alpha + \beta| \\ &= |\nu(A) + \nu(B)| \\ &= |AB| \end{aligned} \tag{19}$$

and $\dim(X+Y) = d$. We therefore have

Corollary 15. *Let A, B, and d be as above. Then we have*

$$|AB| \geq |B| + d|A| - \frac{d(d+1)}{2}. \tag{20}$$

Now, since $\dim(X+Y) \leq \dim(X) + \dim(Y)$, we have $|A| + |B| = |X| + |Y| \geq d + 2$. We can now derive

Lemma 16. *Let A, B, and d be as above, and let $K \geq 1$ be such that $|A| + |B| \geq K(d+2)$. Let $m = \max(\dim_\times(A), \dim_\times(B))$. Then*

(a) If $K > C \geq 1$ we have

$$m < \frac{\alpha - C}{1 - \frac{C}{K}} \tag{21}$$

(b) If $C < 1$, we have

$$m < \frac{(\alpha - 1)}{C\left(1 - \frac{1}{K}\right)} \tag{22}$$

Proof. Since AB contains (multiplicative) translates of both A and B, we see that $d \geq \max(\dim_\times(A), \dim_\times(B))$.

(a): If $C \geq 1$, then by Corollary 15 we have

$$\alpha|A| > |AB| \geq |B| + d|A| - \frac{d(d+1)}{2}.$$

Rearranging,

$$\alpha \geq C + d - \frac{d(d+1)}{2|A|}.$$

Now, we have $2C|A| = 2|B| > |A| + |B|$, so this gives

$$\alpha - C \geq d - \frac{Cd(d+1)}{K(d+2)}$$

and we see the result.

(b): If $C < 1$, then

$$\alpha|A| > |A| + d|B| - \frac{d(d+1)}{2}.$$

Hence

$$\frac{1}{C}(\alpha - 1) > d - \frac{d(d+1)}{2C|A|}$$

and substituting for $2C|A|$ in the last term we have the result.

□

The singular behaviour when $K = C$ or $K = 1$ will not be a problem for the application, as the following lemma shows.

Lemma 17 (Multiplicative bases have large productset)**.** *Let d be a large integer. Suppose that $X, Y \subset \mathbb{R}^d$ satisfy $|Y| = C|X|$, $C \leq \log|X|$, and $\dim(X + Y) = d$. Set $|X| + |Y| = K(d + 2)$. Then if $K \leq \log|X|$ we have*

$$|X + Y| \geq |X||Y|/(2^{10}\log^2|X|). \tag{23}$$

Proof. Since $\dim(X \cup Y) \geq \dim(X + Y)$, there are linearly independent vectors $x_1, \ldots, x_r$ and $y_1, \ldots, y_{d-r}$ for some $1 \leq r \leq d$ and points x_0, y_0 such that $x_0 + x_i \in X$ for $1 \leq i \leq r$ and $y_0 + y_j \in Y$ for $1 \leq j \leq d - r$.

First, suppose that $r \geq d/2$. Then let Y' be any subset of Y with $|Y'| = \lfloor |Y|/(16\log|X|)\rfloor$. Note that $|Y| \geq |X|$, so $|Y'| \neq 0$, but

$$|Y'| \leq (d + 2)/8 = d/8 + 1/4 \leq d/4.$$

Hence we may choose $X' \subset \{x_1, \ldots, x_r\}$ such that $|X'| = \lfloor d/4\rfloor \geq |X|/(16\log|X|)$ and such that the spans of X' and Y' do not intersect. Since $x + y = x' + y'$ forces $y - y' = x' - x$, it follows that

$$|X + Y| \geq |X' + Y'| \geq (|X|/(2^5\log|X|))(|Y|/(2^5\log|X|)).$$

If $r \leq d/2$, then $d - r \geq d/2$, and the argument is the same with the sets exchanged. □

Since we have assumed that $\alpha, C < \log |A|$, we can use Lemma 17 with the assumption on $|AB|$ to bound K away from C when $C \geq 1$, and away from 1 when $C < 1$. To proceed we begin by noting the following analogy of 11.

Lemma 18 (Cauchy-Schwartz for sumsets of distinct sets)**.** *Let M denote the number of additive $2(k+l)$-tuples in $A^{2k} \times B^{2l}$. Then*

$$|kA + lB| \geq \frac{|A|^{2k}|B|^{2l}}{M} \tag{24}$$

Proof. Let $r_{kA+lB}(x) = |\{(a_1+\cdots+a_k+b_1+\cdots+b_l) \in A^k \times B^l : a_1+\cdots+a_k+b_1+\cdots+b_l = x\}|$. Then by the Cauchy-Schwartz inequality we have

$$\begin{aligned} |A|^{2k}|B|^{2l} = \sum_{x \in kA+lB} r_{kA+lB}(x) &\leq |kA+lB|^{1/2} \left(\sum_{x \in kA+lB} (r_{kA+lB}(x))^2 \right)^{1/2} \\ &= |kA+lB|^{1/2} M^{1/2} \end{aligned} \tag{25}$$

□

Using Chang's version of the induction lemma with $A \cup B$, we can immediately obtain a version of Theorem 3 provided that C is absolutely bounded. If we wish to obtain the finer control over C, however, we must refine the argument by proceeding through the proof of the lemma while remaining attentive to which variables lie in A and which lie in B.

We define γ_0, γ_1, and $D_{t,m}$ as we did in the proof of Lemma 9. We summarize the following additivity properties for use in the sequel.

Lemma 19 (Additivity properties of γ_0 and γ_1)**.** *For positive integers k, l such that $k + l > 2$ we have*

(a) $\gamma_1(k+l-1) = \gamma_0(k+l) - 1$

(b) If $k, l \geq 2$ and k, l are not both odd, then $\gamma_1(k+l-1) = \gamma_0(k) + \gamma_0(l) - 1$.

(c) $\gamma_0(k) + \gamma_1(l) \leq \gamma_1(k+l)$

Proof. We may compute all three directly by separating into cases based on the parity of k and l. □

Let

$$\mu_0(k+l) = \begin{cases} C^{\lfloor l/2 \rfloor} D_{k+l,m} |A|^{\gamma_0(k+l)}, & \text{if } k+l \text{ is odd} \\ C^{\lfloor l/2 \rfloor} |A|^{\gamma_0(k+l)} + C^{\lfloor l/2 \rfloor} D_{k+l,m} |A|^{\gamma_0(k+l)-1}, & \text{if } k+l \text{ is even} \end{cases}$$

$$\mu_1(k+l) = \begin{cases} C^{\lfloor l/2 \rfloor} |A|^{\gamma_1(k+l)} + C^{\lfloor l/2 \rfloor} D_{k+l,m} |A|^{\gamma_1(k+l)-1}, & \text{if } k+l \text{ is odd} \\ C^{\lfloor l/2 \rfloor} D_{k+l,m} |A|^{\gamma_1(k+l)}, & \text{if } k+l \text{ is even} \end{cases} .$$

We can now prove:

Lemma 20 (Small multiplicative dimension implies few solutions)**.** *Suppose $A, B \subset K$ satisfy $A = -A, B = -B$, and $0 \notin A \cup B$. Let $m = \max(\dim_\times(A), \dim_\times(B))$. Set $|B| = C|A|$. For $k, l \in \mathbb{N}$, let $\sigma_0(k,l)$ denote the number of solutions to $a_1 + \cdots + a_k + b_1 + \cdots + b_l = 0$ and let $\sigma_1(k,l)$ denote the number of solutions to $a_1 + \cdots + a_k + b_1 + \cdots + b_l = 1$.*

(a) $\sigma_0(k,l) \leq \mu_0(k+l)$

(b) *In addition, if $k, l \geq 2$ are not both odd, then for $k+l$ odd we have*

$$\sigma_0(k,l) \leq D_{k+l,m} C^{\lfloor l/2 \rfloor} |A|^{\gamma_0(k)+\gamma_0(l)-1}$$

and for $k+l$ even we have

$$\sigma_0(k,l) \ll_{k+l} C^{\lfloor l/2 \rfloor} |A|^{\gamma_0(k)+\gamma_0(l)} + C^{\lfloor l/2 \rfloor} D_{k+l,m} |A|^{\gamma_0(k)+\gamma_0(l)-1}.$$

(c) $\sigma_1(k,l) \leq \mu_1(k+l)$

Proof. We may assume that $k, l > 0$ since the remaining cases are covered by the version of Lemma 9 in [4].

Base Case: When $k = 1, l = 1$, we see that the number of solutions to $a_1 + b_1 = 0$ is at most $|A|$ (Each of $|A|$ choices for a_1 gives one possibility for b_1). Meanwhile, the number of nondegenerate solutions to $a_1 + b_1 = 1$ is at most $\exp((12^6(2m+1))$ by Theorem 4, and the only two possible degenerate solutions are $(0,1)$ and $(1,0)$. We have

$$\exp((12)^6(2m+1)) + 2 \leq \exp(2^{24}(m+1)).$$

Hence the bound holds for $k + l = 2$.

Induction: Fix $k, l \in \mathbb{Z}^+$, and suppose that all parts of the lemma have been proved for pairs k', l' with $k' + l' < k + l$.

(a): We can rewrite $a_1 + \cdots + a_k + b_1 + \cdots + b_l = 0$ as $a'_2 + \cdots + a'_k + b'_1 + \cdots + b'_l = 1$, where the variables a'_i, b'_j are constrained to sets of size $|A|$ and $|B|$ respectively (with no change in multiplicative dimension), by fixing a value of $-a_1$, dividing through by it, and rearranging. By the inductive hypothesis, this new equation has fewer than $\mu_1(k+l-1)$ solutions, whereby our target equation has at most

$$|A|\mu_1(k+l-1) \leq \mu_0(k+l)$$

by Lemma 19 (a), as desired.

(b): Let $k, l \geq 2$, k and l not both odd. We proceed exactly as above, but apply Lemma 19 (b) to $\mu_1(k+l-1)$ to obtain the result.

(c): To count solutions to $a_1 + \cdots + a_k + b_1 + \cdots + b_l = 1$, we begin by applying the Theorem 4. This tells us that the number of nondegenerate solutions in the entirety of the group $G_A^k \times G_B^l$ is bounded by $\exp(6(k+l)^{3(k+l)}((k+l)m+1))$.

We use the inductive hypothesis to count degenerate solutions. This reduces to computing, for each quadruple $k_1, l_1, k_2, l_2 \in \mathbb{Z}^+$ such $k_1+k_2 = k$, $l_1+l_2 = l$, and $k_1+l_1 \geq 2$, the number of solutions to the pair of equations

$$\sum_{r=1}^{k_1} a_{i_r} + \sum_{r=1}^{l_1} b_{j_r} = 0$$

$$\sum_{r=k_1+1}^{k} a_{i_r} + \sum_{j=l_1+1}^{l} b_{j_r} = 1$$

where $i_1, \ldots, i_k$ is some permutation of $1, \ldots, k$ with $i_1 < \cdots < i_{k_1}$ and $i_{k_1+1} < \cdots < i_k$, and $j_1 \ldots, j_l$ is some permutation of $1, \ldots, l$ with $i_1 < \cdots < i_{l_1}$ and $i_{l_1+1} < \cdots < i_l$.

The number of solutions is therefore bounded by

$$2 \sum_{k_1, l_1} \binom{k}{k_1}\binom{l}{l_1} \mu_0(k_1 + l_1)\mu_1(k_2 + l_2)$$

where again we have used the extra factor of two to account for the nondegenerate solutions.

Now, if $k + l$ is odd, then we either have $k_1 + l_1$ even and $k_2 + l_2$ odd, in which case

$$\mu_0(k_1 + l_1)\mu_1(k_2 + l_2) \leq \mu_1(k + l)$$

by an application of Lemma 19 (c), or else $k_1 + l_1$ is odd and $k_2 + l_2$ is even, in which case

$$\mu_0(k_1 + l_1)\mu_1(k_2 + l_2) \leq \frac{k + l - 3}{2} < \mu_1(k + l).$$

We note that to combine the constants $D_{k_1+l_1,m} D_{k_2+l_2,m}$ here we have set $t = k_1 + l_1$, so $k_2 + l_2 = k + l - t$, and have used the analysis from Lemma 9. The result now follows for $k + l$ odd on factoring out $\mu_1(k + l)$ and computing $\sum_{k_1,l_1} \binom{k}{k_1}\binom{l}{l_1} = 2^{k_1+l_1}$.

If $k+l$ is even, we proceed similarly, however in each decomposition k_1+l_1 and k_2+l_2 will have identical parity, leading to the loss of exponent in $\mu_1(k + l)$.

The result now follows by induction.

□

Now, for arbitrary sets $A, B \subset K$ satisfying $|AB| < \alpha|A|$, we may apply Lemma 20 to $A' = (A \cup (-A)) \setminus \{0\}$ and $B' = (B \cup (-B)) \setminus \{0\}$. As in Section 2, we may then bound the number of solutions gained by adding 0 back to A and B. The numerics are identical to those previous, and the final result is

Lemma 21 (Additive tuples in distinct sets)**.** *Let* $A, B \subset K$ *satisfy* $|B| = C|A|$ *and* $|AB| < \alpha|A|$. *Then the number of additive* $2k+2l$*-tuples* M *in* $A^{2k} \times B^{2l}$ *satisfies*

$$M \ll_{k+l} |A|^k|B|^l + e^{((k+l)^{65(k+l)}\alpha)}|A|^{k-1}|B|^l$$

if $C \geq 1$ *and*

$$M \ll_{k+l} |A|^k|B|^l + e^{((k+l)^{65(k+l)}\frac{\alpha}{C})}|A|^{k-1}|B|^l$$

if $C < 1$.

Theorem 3 now follows by Lemma 18.

References

[1] M.-C. Chang. A polynomial bound in Freiman's theorem. *Duke Math. J.*, 113:399–419, 2002.

[2] M.-C. Chang. Erdös-Szemerédi problem on sum set and product set. *Ann. of Math.*, 157:939–957, 2003.

[3] M.-C. Chang. On sums and products of distinct numbers. *J. Combin. Theory Ser. A*, 105(2):349–354, 2004.

[4] M.-C. Chang. Sum and product of different sets. *Contrib. Discrete Math.*, 1(1):47–56, 2006.

[5] P. Erdös and E. Szemerédi. On sums and products of integers. In *Studies in Pure Mathematics*, pages 213–218. Birkhauser, Switzerland, 1983.

[6] J.-H. Evertse, H.P. Schlickewei, and W.M. Schmidt. Linear equations in variables which lie in a multiplicative group. *Ann. of Math.*, 155(3):807–836, 2002.

[7] I. Z. Ruzsa. Sum of sets in several dimensions. *Combinatorica*, 14(4):485–490, 1994.

[8] I. Z. Ruzsa. Sums of finite sets. In *Number Theory (New York, 1991-1995)*. Springer-Verlag, New York, 1996.

[9] T. Tao and V. Vu. *Additive Combinatorics*. Cambridge University Press, Cambridge, UK, 2006.